UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/929,121	08/15/2001	Toyoaki Kishimoto	212668US6	1335

22850 7590 08/23/2005

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER
TESLOVICH, TAMARA

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 08/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

## *Office Action Summary*	**Application No.** 09/929,121	**Applicant(s)** KISHIMOTO, TOYOAKI	
	Examiner Tamara Teslovich	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 May 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments filed May 18, 2005 have been fully considered but they are not persuasive.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Applicant submits that the Examiner has failed to make a *prima facie* case of obviousness, because neither Levergood nor Ericsson, alone or in combination, teach or suggest the claimed registering step, decoding step, or determining step.

The Examiner would like to draw attention to page 4, lines 16-19 of Applicant's remarks wherein Applicant concedes that "Levergood describes that information such as client IP address and password, as well as user demographic information, such as user age, home address, hobby or occupation may be stored in the content server" and that "such information may be considered unique identification information". Examiner would also like to draw attention once again to Levergood column 3, lines 21-43 wherein Levergood teaches wherein "a client's request is redirected to an authentication server" which then "interrogates the client" for unique identification information so that it might register the client, or "open a new account" within an "account database 216" and if accepted, issue an SID to be used in future communications.

Official notice is taken of the capabilities of internet browsers at the time of the invention, namely those associated with the caching of unique identification information to be utilized at a later time for purposes of identification and authentication. It would have been considered common knowledge to one of ordinary skill in the art at the time of the invention that the majority of browsers in use by clients came loaded with the abovementioned capabilities, those browsers including but not limited to Internet Explorer 5.x which by default is configured to remember everything typed.

The Applicant goes on to argue that Levergood fails to teach or suggest the decoding of the unique identification information encrypted by a predetermined encryption algorithm and supplied from said mobile information terminal via said open network. The first paragraph of column 7 of Levergood teaches the use of GET and POST URL messages in order to transmit personal information and credit reference from the client to the authentication server. It is common knowledge to one of ordinary skill in the art at the time of the invention that the HTTP 1.1 specification utilizes "chunked encoding" to transfer data to remote servers when using the POST command in addition to the optional MIDP application/x-www-form-urlencoded MIME type which affords additional encoding capabilities.

In response to part three of Applicant's original argument regarding Levergood's supposed failure to disclose "determining whether the unique identification information decoded in the decoding step is registered with said customer database", the Examiner would like to draw attention to column 3 of Levergood, lines 29-32: "Upon receiving a redirected request, the authentication server returns a response to interrogate the client and then issues an SID to a *qualified* client." See also column 6 lines 36-65, wherein Levergood teaches that "the authentication server sends a "CHALLENGE" response which causes the client browser to prompt the user for credentials" so that a GET requests may be sent to the authentication server which then "queries an account database to determined whether the user is authorizes to access the requested document" and wherein "a preferred account database may contain a user profile which includes information for identifying purposes, such as a client IP address and password, as well as user demographic information, such as user age, home aggress, hobby, or occupation, for later use by the content server."

The Applicant further submits that Ericsson fails to teach or suggest the abovementioned features of claim 1 and requests that the 35 U.S.C. 103 rejections be withdrawn for claims 1 and 9. The Examiner maintains the arguments set forth above in regards to Levergood and agrees with the Applicant's observation that Ericsson describes the ability of a mobile phone to connect over the internet to a server device, which is why it has been combined with the Levergood reference for the Examiner's rejections.

In view of the arguments previous, Examiner respectfully disagrees with the Applicant's argument that the combination of Levergood and Ericsson fails to disclose claim 1 in its entirety, and maintains the 35 U.S.C. 103 rejections corresponding to claims 1-6.

For substantially the same reasons as given with respect to claims 1-6, the Examiner maintains the 35 U.S.C. 103 rejections corresponding to claims 9-10.

With respect to claims 7, 8, 11, and 12, Applicant reiterates the same arguments applied to claims 1-6 and 9-10 above, adding that Wan fails to remedy the deficiencies of Levergood and Ericsson. For the reasons given above, Examiner maintains that the combination of Levergood and Ericsson does in fact teach all the claim limitations, thereby supporting the 35 U.S.C. 103 rejections corresponding to claims 7, 8, 11, and 12.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-6, and 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Levergood et al. (US Patent 5,708,780) further in view of Ericsson.

Regarding Claim 1, Levergood et al. teaches a user authentication method for an authentication server which executes user authentication between a [client] and a content providing server interconnected by an open network not guaranteeing the security of data to be transferred, comprising the steps of:

registering unique identification information stored in said [client] with a customer database of said authentication server in advance (see column 3 lines 21-43);

decoding the unique identification information encrypted by a predetermined encryption algorithm and supplied from said [client] terminal via said open network (see col.7 paragraph 1);

determining whether the unique identification information decoded in the decoding step is registered with said customer database (see col.3 lines 29-32; col. 6 lines 36-65); and

sending a notification to said content providing server that starting of service provision for said [client] be permitted, if the unique identification information is found registered with said customer database in the determining step (see col.3 lines 43-48 reference ""content server receives a URL request accompanied by an SID").

Levergood et al. fails to teach the abovementioned system wherein the client is a "mobile information terminal".

Ericsson teaches the important of "enabling users of PCs connection to the Internet via mobile telephones, handheld devices, and smartphones to download Web pages more quickly" (see Ericsson).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Levergood et al. the wireless capabilities as described in Ericsson to provide for users connected to the Internet via mobile information terminals or handheld devices.

Regarding Claim 2, the combined method of Levergood et al. and Ericsson teaches the user authentication method according to Claim 1, further comprising the step of:

presenting, to said mobile information terminal, a recommended menu including site access information for accessing a plurality of predetermined content providing servers (see Levergood et al. col.8 lines 27-58 reference “”customize user requested pages to include personalized content”);

wherein a process in which site access information selected by a user of said mobile information terminal from said recommended menu displayed on said mobile information terminal is registered with said customer database in relation with the unique identification information of said mobile information terminal is included in the registering step (see Levergood et al. col.4 lines 32-42).

Regarding Claim 3, the combined method of Levergood et al. and Ericsson teaches the user authentication method according to Claim 2, wherein, in the registering step, when registering said site access information with said customer database, user authentication is performed on the basis of said unique identification information before this registration and said mobile information terminal requested to make display for prompting said user to enter a password of the user (see Levergood et al. col.6 lines 44-49 reference “causes the client browser to prompt the user for credentials, a preferred credential query typically consists of a request for user name and password”), while, subsequent to the registration with said customer database, an access request is made on the basis of the site access information already registered with said customer database, the user authentication on the basis of said unique identification information is performed but the request for the display for prompting the user to enter the user's password is omitted (see Levergood et al. col.6 lines 40-44 reference “forgo the credential check procedures”).

Regarding Claim 4, the combined method of Levergood et al. and Ericsson teaches the user authentication method according to Claim 3, wherein, in the registering step, a charging server is instructed to charge said user for the use of a service provided by said content providing server associated with said site access information at the time of registering said site access information with said customer database (see Levergood et al. col.9 lines 1-6 reference “a user may be charged and billed each time she accesses a particular document through the internet”).

Regarding Claim 5, the combined method of Levergood et al. and Ericsson teaches the user authentication method according to Claim 4, wherein, in the registering step, a confirmation step for confirming, before instructing said charging server for the charging, that said user is a registered user of said charging server is included (see Levergood et al. col.9 lines 1-6).

Regarding Claim 6, the combined method of Levergood et al. and Ericsson teaches the user authentication method according to claim 1, wherein said open network is the Internet, through which the unique identification information is transmitted as encrypted by the predetermined encryption algorithm by a Web browser installed on said mobile information terminal (see Levergood et al. col.3 lines 8-23).

Regarding Claim 9, Levergood et al. teaches a user authentication server which executes user authentication between a [client] and a content providing server interconnected by an open network not guaranteeing the security of data to be transferred, comprising:

registering means for registering unique identification information stored in said [client] with a customer database of said authentication server in advance (see column 3 lines 21-43);

decoding means for identification information decoding the unique encrypted by a predetermined encryption algorithm and supplied from said [client] via said open network (see col.7 paragraph 1);

determining means for determining whether the unique identification information decoded by the decoding means is registered with said customer database (see col.3 lines 29-32; col. 6 lines 36-65); and

service permission notice sending means for sending a notification to said content providing server that starting of service provision for said [client] be permitted, the unique identification information is found registered with said customer database by the determining means (see col.3 lines 43-48 reference “”content server receives a URL request accompanied by an SID”).

Levergood et al. fails to teach the abovementioned system wherein the client is a “mobile information terminal”.

Ericsson teaches the important of “enabling users of PCs connection to the Internet via mobile telephones, handheld devices, and smartphones to download Web pages more quickly” (see Ericsson).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Levergood et al. the wireless capabilities as described in Ericsson to provide for users connected to the Internet via mobile information terminals or handheld devices.

Regarding Claim 10, teaches the user authentication server according to Claim 9, wherein said open network is the Internet, through which the unique identification information is transmitted as encrypted by the predetermined encryption algorithm by a Web browser installed on said mobile information terminal (see Levergood et al. col.3 lines 8-23).

Claims 7, 8, 11, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Levergood et al. (US Patent 5,708,780) and Ericsson as applied to Claims 1-6 and 9-10 above, and further in view of Wan (US Patent 6,044,069).

Regarding Claim 7, the combined method of Levergood et al. and Ericsson teaches the user authentication method according to Claim 6, wherein unique identification information is read, by said Web browser, from said mobile information terminal and the retrieved unique identification information is transmitted as encrypted by the predetermined encryption algorithm by said Web browser.

Levergood et al. and Ericsson fails to teach the abovementioned method wherein the unique identification information is read from a flash memory installed on said mobile information terminal.

Wan teaches the use of flash memory in mobile information terminals for the purpose of storing non-volatile information (see Wan reference "mobile station identifier" and "flash").

It would have been obvious to a person of average skill in the area at the time of the invention to include within Levergood et al. and Ericsson the flash storage and retrieval of information as described in Wan to provide users with memory that is quieter, faster, smaller, lighter, and non-volatile.

Regarding Claim 8, the combined method of Levergood et al., Ericsson, and Wan teaches the user authentication method according to Claim 7, wherein said predetermined encryption algorithm is SSL (Secure Socket Layer) (see Ericsson reference "Netscape Navigator" and "Microsoft Internet Explorer" both of which utilize a version of SSL, and "WAP" which utilizes TSL, a version of SSL).

Regarding Claim 11, the combined method of Levergood et al. and Ericsson teaches the user authentication server according to claim 10 wherein unique identification information is read, by said Web browser from said mobile information terminal and the retrieved unique identification information is transmitted as encrypted by the predetermined encryption algorithm by said Web browser (see Wan).

Levergood et al. and Ericsson fails to teach the abovementioned method wherein the unique identification information is read from a flash memory installed on said mobile information terminal.

Wan teaches the use of flash memory in mobile information terminals for the purpose of storing non-volatile information (see Wan reference "mobile station identifier" and "flash").

It would have been obvious to a person of average skill in the area at the time of the invention to include within Levergood et al. and Ericsson the flash storage and retrieval of information as described in Wan to provide users with memory that is quieter, faster, smaller, lighter, and non-volatile.

Regarding Claim 12, the combined method of Levergood et al., Ericsson, and Wan teaches the user authentication server according to claim 11 wherein said predetermined encryption algorithm is SSL (see Ericsson reference "Netscape Navigator" and "Microsoft Internet Explorer" both of which utilize a version of SSL, and "WAP" which utilizes TSL, a version of SSL).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T. Teslovich
August 12, 2005

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER